KOREAN AIR LINES FLIGHT 007:
LESSONS FROM THE PAST AND INSIGHTS FOR THE FUTURE

Asaf Degani

NASA Ames Research Center,
Mountain View, California
adegani@mail.arc.nasa.gov

INTRODUCTION

Pilot interaction with automated systems such as autopilots and Flight Management Systems is a thorny flight safety issue (Abbott, Slotte, and Stimson, 1996). This issue will only grow in importance and visibility as more and more automated systems, including state-of-the-art information systems and flight guidance systems, are introduced on the flight deck. The majority of the problems pilot encounter when using automated systems center around two factors: (1) the pilot has an incomplete and inadequate model of how the autopilot works; and (2) the displays and flight manuals, provided to the pilot, are inadequate for the task (Woods, Sarter, and Billings, 1997).

The tragic accident of Korean Air Lines Flight 007, a Boeing 747 that deviated from its intended flight path, provides a compelling case-study of problems related to pilots' use of automated systems. This paper describes what had happened and exposes two types of human-automation interaction problems: (1) The pilots of KAL were not provided with adequate information about the actual behavior of the autopilot and its mode transition logic; and (2) The autopilot onboard KAL 007 did not provide adequate information to the flight crew about its active and armed modes. Both factors, according to the International Civil Aviation Organization (1993) report on the accident, contributed to the aircraft's lethal navigation error.

Almost 20 years later, the same types of problems still exist in today's automated aircraft. Pilots continue to report situations in which the automation does not behave in the way they expect it. Pilots report of cases where they do not understand "what the automation is doing, why is it doing it, and what will it do next" (Wiener, 1989). This paper describes an systematic approach for understanding these types of deficiencies in the design of modern automated systems. Methodologies for identifying such problems in the design of automated systems are currently been developed and tested (Degani and Heymann, in press)

FLIGHT 007

One of the most tragic aviation accidents in the 20th century was the destruction of a Korean jetliner in 1983 Korean Air Lines Flight 007 (KAL 007), a Boeing 747 jumbo jet flying from Anchorage, Alaska, to Seoul in South Korea, deviated more than 200 miles from its intended flight route into Soviet territory and was shot down. There were no survivors; all 240 passengers and 29 crewmembers perished. Figure 1 is a picture of this aircraft.

==========

Figure 1. Korean Air Lines Boeing 747

==========

Following the downing of the aircraft, Russian military vessels searched for the aircraft wreckage. Two month later, Soviet divers, operating out of a civilian drilling ship, brought up the aircraft's "black boxes" – the cockpit's voice recorder and the digital flight data recorder. The Soviets analyzed the recorders to find clues to the accident, but kept their findings secret. Ten years later, after the collapse of the Iron Curtain, the tapes were handed over to the International Civil Aviation Organization (the civil aviation arm of the United Nations Organization) for analysis. The accident investigation was completed in 1993; the discussion in this chapter is based primarily on the report of the ICAO investigative team.

The date is August 31, 1983. Location: Anchorage airport. After a long takeoff roll, Korean Airlines Flight 007 pitched up and climbed slowly into the morning sky. The

crew was instructed to change the aircraft direction (heading), and the aircraft gently rolled to the left. Flight 007 was then given the following air traffic control directive: fly directly to the *Bethel* navigational beacon and then follow transoceanic route (R-20) all the way to Seoul. Shortly after, the aircraft slowly deviated to the right (North) of its intended route. It first passed 6 miles north of the *Cairn Mountain* (navigational) way-point, then 12 miles north of the *Bethel* way-point (see Figure V-2). Slowly but steadily, the rift between the route and the actual location of the aircraft grew. At half past five in the morning, local time, the weary passengers on this westbound flight, which had originated from New York City, were fast asleep. In the cockpit, the flightcrew were tracking the flight, passing over NABIE, NUKKS, NEEVA, NINNO, NIPPI, NYTIM, NOKKA, and NOHO -- a sequence of navigation way-points over the cold Bering Sea on route to Seoul.

Everything looked normal.

But it really wasn't. As the flight progressed across the vast ocean, the divergence between the actual aircraft path and the intended flight route increased. Several hours after takeoff from Anchorage, the rift was more than 150 miles wide, and now the aircraft had strayed into an airspace closely monitored by the Soviets. The aircraft was heading toward USSR territory. It was silently being tracked by the Soviets.

==========

Figure 2. Flight path of Korean Air Lines 007

==========

At the time, a United States Air force Boeing RC-135, the military version of the four-engine commercial Boeing 707, was flying a military reconnaissance mission, code name "Cobra Dane," over an area East of the Kamchatka Peninsula. The Korean Boeing 747, also a four-engine aircraft, was flying off-course directly toward this location. The geographical proximity between the meandering Korean Air Lines Boeing-747 and the orbiting military aircraft led the Soviet air-defense personnel sitting in front of their radar screens to assume that the target moving steadily toward Siberia was a military aircraft, probably the Boeing RC-135. They initially designated it as an "unidentified" target.

When the Korean jetliner was about 80 miles from the Kamchatka coast -- a narrow peninsula, filled with active volcanoes that extends from Siberia to the Bearing Sea -- four MiG-23 fighters were scrambled to intercept it. The fighters flew to the east for the intercept, then turned west and started a chase to reach the fast and high-flying Boeing 747. Unable to close in on the target, the MiG-23's were instructed to return to base. The Korean jetliner, now 185 miles off course, crossed over Kamchatka peninsula and into the Sea of Okhotskand. Over international waters, safe for the moment, the large aircraft was heading toward another Soviet territory, Sakhalin Island.

Approaching Sakhalin Island from the northeast, two Soviet (Su-15) fighters were scrambled from the Sokol Airbase toward the target. On the radar screen inside the military air-defense control center, the civilian airliner was now designated as a military target, most likely an American RC-135 on an intended intrusion mission. Because of this designation, the rules for identification and engagement employed by the Soviet air-defense command in this particular case were those reserved for military action against Soviet territory (and not the international rules for civil aircraft straying into sovereign airspace). Apparently, there had been more than a few such intrusions into Soviet airspace in the preceding months, to the annoyance of the Soviet military establishment. An order was given to air-defense commanders that the contact was a combat target that was to be destroyed if it violated the State's borders, again.

About 20 minutes later, Flight 007 crossed into the airspace of Sakhalin Island, a well-guarded island with many sensitive military installations. The flight crew had no idea they were entering a hornet's nest. Flying at 33,000 feet, the pilots were engaged in a casual conversation in the cockpit and over the radio with another Korean Air Lines aircraft also abound for Seoul. But outside the warm and well-lit cockpit, a sliver Soviet fighter jet was screaming through darkness for an intercept. The fighter made visual contact, and was now trailing about 4 miles behind the big aircraft. The fighter pilot saw the aircraft lights, but because of the early morning darkness, he was unable to identify what kind of an aircraft it was.

When asked by his ground controller, the pilot responded that there are four (engine) contrails. This information matched the air-defense command assumption that this was indeed an American RC-135, also with four engines, on an intrusion mission into Soviet territory. Meanwhile, the crew of KAL 007 – completely unaware of the ongoing intercept and the tension within the Soviet air-defense command – were establishing routine radio contact with Tokyo Air Traffic Control. And then they made a casual request with Tokyo Control to climb to an altitude of 35,000 feet.

The fighter pilot, in response to his controller's command, flashed his lights, and fired a burst of 200 bullets below the jetliner as a warning (hoping to force the aircraft to land at Sakhalin). The round of bullets did not include tracer bullets; and in the vast darkness, the bullets were not seen or heard. The entire chase, intercept, and the firing was not noticed by the crew of Korean Air Lines Flight 007, flying at night with window shades lowered.

The fighter pilot reported to his controller that he had flashed his lights and fired a warning burst. At the same moment, KAL-007 received the response from Tokyo air traffic control: "climb and maintain 35,000 feet." The 747 began a gradual climb to a higher altitude. The fighter was now almost abeam the aircraft. Soviet ground controllers were engaged in stressful communications with their supervisors about what to do. Crossing the southern part of Sakhalin Island, the jetliner was about to coast out of Soviet territory back into the sea. However, beyond the Sea of Japan lay mainland Russia and the naval base of Vladivostok, the home of the Soviet's most sensitive nuclear and naval installations. Air defense controllers asked if the enemy target was descending. The fighter pilot first reported that the target was flying level and was reducing its speed. Then came the report that he was falling behind the target.

"Engage afterburners and destroy the target!"

The fighter pilot got into attack position and engaged full thrust. Seconds later, he launched two air-to-air missiles toward the target. At least one missile exploded near the vulnerable, high-flying jet. The aircraft first pitched up. The blast caused a loss of pressure inside the large cabin. The flight engineer gave repeated orders to don the

yellow oxygen masks. Then the aircraft started to descend and roll to the left. The Captain and First Officer tried helplessly to control the aircraft and arrest its downward spiral. Two minutes later, the aircraft stalled, out of control, over the water. It crashed into the sea, about 20 miles off the Sakhalin coast.

WHY DID THE AIRCRAFT STARY FROM COURSE?

Two minutes and 10 seconds after liftoff, according to the flight data recorder, the pilots engaged the autopilot. The aircraft was flying under autopilot command until it was hit 5 hours later. As many suspected from the very beginning, the autopilot system, or more accurately pilot interaction with the autopilot system, holds an important clue to the navigation fiasco.

When the pilot engaged the autopilot, the active mode was HEADING. In HEADING mode, the autopilot simply maintains the selected heading, which initially was 220 degrees (southwesterly). After receiving a directive to fly to *Bethel* waypoint, the pilot rotated the "heading select knob" and changed the heading to 245 degrees (see Figure 3(a)). The autopilot maintained this dead-reckoning heading with extreme precision until the aircraft was fired upon hours later. Additionally, the pilot can select a mode called INS NAVIGATION, by rotating the autopilot mode selector to the right (see Figure 3(b)). When INS NAVIGATION becomes the active mode, the autopilot follows inputs from the Inertial Navigation System (INS), a dedicated computer that computes the aircraft path's along the navigation route (based on a sequence of navigational waypoints previously entered by the pilot).

=========

Figure 3. Mode selector and annunciations

=========

The Inertial Navigation System sends steering commands to the autopilot, and the autopilot flies the aircraft accordingly along the route of flight. On this flight, the route was transoceanic route R-20 with some 10 waypoints, passing very close to, yet shy of, of Soviet-monitored airspace. To comfortably fly the aircraft along R-20 to Seoul, the pilots should have engaged the autopilot in INS NAVIGATION mode. This was the

norm and in accordance with Korean Air Lines procedures. It did not happen on this flight. Instead, as mentioned earlier, the autopilot maintained a constant heading of 245 degrees until the aircraft was struck by missiles.

THE AUTOPILOT

To understand the internal operations of the autopilot it is necessary to describe its behavior. Here wee shall use a simple state transition notation to construct a simplified description of the autopilot's logic. The initial autopilot mode was HEADING. This is state [1] in Figure V-4(a). Then the pilot selects INS NAVIGATION mode by rotating the switch in Figure V-3(b) to the line labeled "INS NAVIGATION." Now the aircraft should follow the route of flight all the way to Seoul, as was pre-programmed by the pilots. Sounds simple. Actually, it's a bit more complicated, and this was part of the problem. It turns out that several things have to take place before the autopilot *really* goes to INS NAVIGATION mode: One is that the aircraft must be close to the programmed route. Specifically, the distance between the aircraft's actual route and pre-programmed route must be within 7.5 miles for the INS NAVIGATION mode to become active. That's one condition. The other condition is that the aircraft must be flying *toward* the direction of the programmed route (and not, for example, 180 degrees away from it). Only when these two conditions are met, or become TRUE, will the autopilot engage the INS NAVIGATION mode. With these conditions, we introduce the notion of Guards.

==========

Figure 4. autopilot logic and user-model

==========

AUTOMATIC GATE KEEPERS

The autopilot checks for these two entry conditions, by itself, before it completes transition to the INS NAVIGATION mode. This is a routine, automated sequence of steps in the autopilot. This gate keeping routine is called a *guard*. As their name suggests, the role of a guard is to protect a transition. A guard is a logical statement that must be evaluated as true before a transition takes place. Sound complicated?

It's more familiar than you might think. You go into a downtown bar, and there is a hulk of a security guy there, blocking the entrance with his door-wide body, checking young barflies' ages – no ID, no entry. Automatic Teller Machines, ATMs, same story. You can't make an ATM transaction unless you punch in your "...5-digit Personal Identification Number." All said and done, the PIN is a guard. Unless you supply the correct card and the correct PIN, you are locked, or guarded, out.

Now back to the autopilot and its guards. We said that we have two conditions: the first says that the lateral distance between the aircraft location and the nearest point on the route must be within 7.5 miles. What we mean by this is that the distance should be equal to or less than 7.5 miles. Right? If the aircraft is 1, 2, 3, 4, 5, 6, 7, or 7.5 miles from the route then we are fine. We express this as

$$\Delta \textit{ distance between [aircraft and INS route]} = < 7.5 \textit{ miles}$$

This logical statement, once evaluated, will produce either a TRUE or FALSE result. The second condition says that the aircraft must be heading toward the route. (There is a mathematical equivalence of this statement, but we should not worry about it now.) We write it in plain English [aircraft is flying toward INS route]. TRUE or FALSE, and we are almost done. You can see these two conditions on the second transition in Figure 4(a).

The guard, the software routine that evaluates whether the transition will fire or not, cares about the first and the second conditions, as well as the *relationship* between them. Any two or more conditions in a guard are tied in a logical relationship. In our case, the relationship is the logical **.and.**, which means that *both* conditions must be evaluated TRUE. What we are saying is that the aircraft must be "at a distance equal or less than 7.5 miles from the INS route" **.and.** "flying toward the direction of the INS route" for the transition to the real INS NAVIGATION to fire. Both conditions must be true, no arguments. Unless you have been checked as a TRUE entrant, you are not allowed in. You have to wait.

Look again at Figure 4(a) and lets retrace the sequence. Initially we are in HEADING mode. This is state [1]. We then decide to engage the INS. Very well. We reach

forward and rotate the mode selector to INS NAVIGATION. This fires the transition to state [2], which is like a waiting room for us. Two conditions must be both TRUE before we can leave the waiting room. We write these two conditions on top of the transition from state [2] to [3]. Now we can finally transition to state [3], which is what we really wanted in the first place. Kind of awkward, isn't it?

This business of a waiting room (state [2]), where we await patiently while the guard checks our entry credentials, begs an interesting question. What does it mean to be in this waiting room? Or more precisely, what does the system do while we are in there? Well, if the conditions on the transition between state [2] and [3] is evaluated as TRUE, then the transition to INS NAVIGATION is instantaneous, and we zip through the waiting room, no problem. But what if any one of the conditions is FALSE? Then, of course, we have to remain in the waiting room. We stay and wait until both conditions are true. But what will the autopilot do in the meantime?

According to this system logic, the autopilot will stay in INS-ARM. What will happen from now on is that each second (the update-rate of the autopilot), the guards evaluate the conditions. TRUE you're in, FALSE – stay out. This will happen over and over (and only stop when the transition to INS NAVIGATION finally fires). All right, we are stuck in INS-ARM, but what does the autopilot do? Which mode is now flying the aircraft? INS NAVIGATION mode is not active and the autopilot therefore gets no steering command from the INS. So what should the autopilot do in the meantime? Well, this is a common dilemma that faces designers of automated control systems: What should one do when conditions have not been met or when certain conditions are no longer valid. In our case, the system cannot transition to the mode that was selected by the pilot, but where should it go?

The designers of this autopilot chose to stay in simple mode, a mode in which the autopilot keeps on maintaining the current heading of the aircraft. When in INS-ARM, the autopilot is actually in HEADING mode. INS-ARM is a limbo mode, on the border, not here and yet not there. It's right there in Figure 4(a), state [2]. The mode is INS-ARM, the display says "INS-ARM," but the autopilot mode is actually in HEADING mode. Was this a factor in this accident? We'll soon see.

AUTOMATIC TRANSITIONS

The transition from INS-ARM to INS NAVIGATION mode is an automatic transition, which means that it has a life of its own: The system may stay in its current mode or switch depending on *external* events outside of the machine (e.g., the distance between the aircraft and the INS route). So who is involved in making this transition take place? It's not only the pilot, is it? No, the transition happens on it own without any direct user involvement; no buttons are pushed and no levers are moved. So who is it? For one, it is whoever wrote the software code for the autopilot. This is where it all begins. And what about the external events (e.g., flying toward the route) that trigger the transition? Some external events can be controlled by the pilot (e.g., by veering the aircraft in the direction of the route) and some (which we have not discussed yet) are triggered by events over which the user may have limited control. The legal responsibility of operating the system has resided traditionally with the operators, the Captain in this case. But is that fair?

Automated systems behave on their own – switching mode and taking action – sometimes doing things that the user did not intend to do. More complex automated systems, with ever more sophisticated automated capabilities, are currently being developed. So who is responsible for what these systems do? Who takes the blame when there is a failure? The answer is not as clear-cut as it used to be in the many centuries of maritime operations and one century of human flight. This is a serious legal matter that is being debated and is still pending in several courts of law, all involving cases of faulty user interaction with complex automation

For now, we need to recognize that what governs the transitions are the *conditions* (written by the designer) on the transitions, and the *events* that trigger them. The user, or pilot in our case, may or may not be fully aware of an entire set of conditions, and he or she may or may not be able to sense and detect the presence of all the events that are being evaluated by the machine. The consequence is clear: if you don't know what will fire the transition, you cannot anticipate it. But is it possible to detail in the operating manual all the conditions on transitions and to provide the pilot with a

display of all the necessary events? Even if we did, can we expect that the user will remember all the conditions and exact numbers at will? Maybe yes, maybe no.

USER-MODEL

To track and monitor what the system is doing, the pilot must have a description, or a model, in his or her head of the system's modes, states, and transitions. And we must realize that this model may at times be incomplete and inaccurate because of poor training and deficient manuals, or simply because the pilot forgets the minute details, especially the numbers. Let us assume for the sake of this discussion that the KAL 007 pilots had an inaccurate user-model about the behavior of this autopilot. Say they knew about going toward the flight route, and that the aircraft needed to be west of Anchorage. Fine. But they only knew that the aircraft must be "near" the route for the autopilot to transition to INS NAVIGATION. And let us quantify this, for the sake of this discussion, by saying that "near" is a distance that is fewer than 20 miles.

Let's take the time and build the model that the user has about the autopilot. Call it the user-model. It has three modes: HEADING, INS-ARM, and INS-NAVIGATION. Transition from HEADING to INS-ARM by rotating the selector, transition from INS-ARM to INS NAVIGATION when the aircraft is "less than 20 miles away the path" and "flying toward it." This is the model shown in Figure 4(b).

By now have two models: the "true" autopilot logic of Figure 4(a) and a user-model of Figure 4(b). Those two models are similar, aren't they, but there are also some differences. To view these differences, let's put one on top of the other and look at the composite model of the two. This is the model in Figure 5(a), which looks a bit different from either the autopilot logic or the user-model we had before. Now to differences: Let's pick all of them up one at a time. First, note that I omitted, for brevity, the *[aircraft is flying toward INS route]* condition in this Figure; we want to focus our attention on the distance condition. Second, you can see in Figure 5(a) that there are now two transitions out of INS-ARM (state [2]); one is going back to INS-ARM and the other to INS NAVIGATION (state [3]).

Why?

First things first: We know for fact that if...

the aircraft's distance from the route is equal or less than 7.5 miles

the transition to INS NAVIGATION will take place. This is the transition between state [2] and [3] in Figure 5(a). This is nothing new, it's the transition that we discussed and showed earlier in the autopilot logic description. Now bring in the user-model (and keep the 20 miles assumption that we made about what the pilots think in the back of your mind). So here we go: The pilots think that anything greater than 7.5 miles and up to 20 miles will *also* trigger the transition to INS NAVIGATION. But we know that this is inaccurate, and that in fact when

the distance between the aircraft and the route is greater than 7.5 miles

.AND.

the distance between the aircraft and the path is less than 20

nothing will happen!

Agree?

The autopilot will simply stay in INS-ARM. So we write this on the transition emanating from state [2] and looping back to it in Figure 5(a).

==========

Figure 5. Composite model

==========

Now let's think about these transitions solely from the pilot's perspective. From his or her perspective, or user-model, the aircraft must be less than 20 miles for the transition to take place. When we superimpose this (pilot) model on the actual machine model we get confused – sometimes the autopilot will transition to INS NAVIGATION and sometimes not.

Think about it this way: if we were to do repeated flights and try to engage the INS system when the distance between the aircraft and the INS route varied between 0 and 20 miles, sometimes we would see transition to INS NAVIGATION and sometimes the autopilot would stay in INS-ARM. To the pilot who has only the "less than 20 miles"

model at his disposal, this will look very erratic; the pilot will not be able to figure out what is going on!

Our pilot is working with a capricious system: it sometimes goes to INS NAVIGATION and sometimes stays in INS-ARM. You can see this right there in Figure 5(b). The same event *(Δ distance between [aircraft, INS path] < 20 miles)* generates two different transition loops. The user, given the model at his or her disposal, cannot anticipate what will happen.

And here is the crux of the entire human-automation story: To be able to track or monitor the behavior of an automated system, the user must be able to anticipate mode changes; this means having accurate information to predict the next mode change, because otherwise the pilot is only there for the ride. To monitor the behavior of the machine, the user must have an *adequate* model, one that allows the user to track the machine along its critical modes. If, on the other hand, the user has at his or her disposal an *inadequate* model, the system will appear capricious, erratic, and uncontrollable.

Ever heard this statement? "Any significantly advanced technology is indistinguishable from magic"? It's a rather famous one by Arthur C. Clarke, the great science-fiction novelist. Magic is all about *not* providing to the viewer all the information necessary to resolve what is happening on the stage – why the rabbit is popping up from a seemingly empty hat, and how the handkerchief disappeared. This is exactly what is being discussed here. The only difference is that we are not in a show – we are not sitting in a plush theater chair and being entertained. Instead, we are trying to control a complex piece of machinery. If we don't provide the pilot with an *adequate* model and knowledge of all the necessary events that trigger system transitions, the autopilot behavior will surprise the pilot. Hence the term "automation surprises" – a situation that is, unfortunately, all too common when pilots interact with today's automated flight-control systems.

BACK TO THE AIR

Now that we understand the essence of automatic behavior and something more about human interaction with it, we can return to the tragic saga of KAL 007 and finish the story, although from here on we are navigating in uncharted territory, because what really happened in that cockpit will never be known completely. The crew engaged the autopilot two minutes or so after takeoff. It was initially in HEADING mode. Two possible sequences of events could have occurred: One, that the crew forgot to select the INS NAVIGATION mode. Two, that the crew selected INS NAVIGATION, but it never engaged.

We'll now follow the more probable scenario, the second one. The crew of Korean Air Lines Flight 007 most probably selected INS NAVIGATION on the mode selector panel once the aircraft was *near* the INS route. This, after all, was the standard operating procedure. They anticipated that the transition to INS NAVIGATION mode would take place and the autopilot would fly route R-20 all the way to Seoul.

It never happened.

Based on radar plots that were analyzed after the accidents, we now know that the actual distance between the aircraft and the INS route was always *greater* than 7.5 miles (Figure 6). And therefore the first condition was FALSE. As the aircraft started to deviate from the intended route, this distance only grew. Every second the guards evaluated the condition, and every time it came back FALSE. The condition stayed like this throughout the flight – the autopilot displaying INS-ARM but actually engaged in HEADING mode and maintaining the 245 magnetic heading all the way to the last tragic moments of Flight 007. The pilots, however, had a different view. According to their model of the autopilot's behavior, the autopilot had indeed transitioned to INS NAVIGATION and was following the programmed route to Korea.

==========

Figure 6 about here

==========

Incidents

Such problems in operating this B-747 autopilot were not new, and the track deviation that resulted was not a fluke or a rare case. There were more than a dozen reported similar incidents in which flight crews selected INS-NAVIGATION mode but did not detect that the INS system was not steering the autopilot. Other incidents involved situations in which flight crews failed to (re) engage ins navigation after using heading mode. Most of these incidents involved track deviations similar to Flight 007, the majority of them resulting in track deviations of less than 60 miles. One incident, however, involved a 250-mile off-track deviation and another one (110 miles) almost resulted a mid-air collision between an off-course El-Al Boeing 747 and a British Airways 747 over the Atlantic Ocean.

Displays

Why did all these experienced flight crews failed to detect that the autopilot was not following the INS route? Fatigue, boredom, forgetfulness? Many factors may have come to play. However, we will focus on our primary topic, pilot interaction with the autopilot. One factor in this context is a divergence between the machine model and the user's model. We already understand how it may have come to be.

The only hope of recovering from such a situation is by getting some feedback from the machine about its actual state and mode, some indication about what the machine is currently doing so that the pilot can recognize that there is a discrepancy between his or her mental model of system operation, what and the system is actually doing. Were there indications about the autopilot's modes in the cockpit? Yes and no. The autopilot has a dedicated display to show the pilot which modes are engaged. The mode display shows when INS-ARM is the active mode and when INS NAVIGATION is engaged (and a few other autopilot modes that are not relevant here). The display, or rather the set of lights, is on the right side of Figure 3(a). This is the YES part of our answer.

The NO regards the HEADING mode. There is no indication when HEADING is engaged, ever. Remember, however, that we are talking here about the early generation of automated control systems, when the importance of human factors in

automation design was hardly considered. Fact. When the autopilot was in INS-ARM, there was no indication that the autopilot was actually maintaining heading. The autopilot was engaged in a limbo mode and the display showed INS-ARM.

Did this lack of mode indication play a role here? Most probably, yes. Did the pilots mistake INS-ARM for INS NAVIGATION? Perhaps. These two indications are very similar in terms of size, location, color and wording (the word INS appears in both). Did the pilots understand the subtle difference between these two modes? Did they know about guards and triggering events and how automatic transitions take place? We'll never know.

What we do know is that the autopilot displays were incomplete by not showing that while INS is armed (INS-ARM), the autopilot is actually in HEADING mode and is maintaining the last input heading. The lack of an indication for the autopilot's active mode deprived the crew of an important visual cue that might have drawn their attention to the fact that the INS NAVIGATION was not engaged. Following the accident, many such autopilots were modified to include this information. In today's autopilot systems, when a system is armed, the display also shows the currently engaged mode; this is now a certification requirement. But this is the blessing of hindsight. This design change came too late to help the crew and passengers of Flight 007.

Many have argued that the crew of Flight 007 was not vigilant. That they did not monitor the INS computer indication, that they did not use their radar to monitor the coastline, and more. This may be true, or not. What *is* true and beyond argument is that in doing their job, they were not supported with proper displays and an adequate user-model.

CONCLUSIONS

It is unnerving to consider that the sequence of actions and coincidences which finally led to the shooting down of a commercial aircraft in which 269 innocent people died, began with something that *didn't* happen – an autopilot mode transition. Many things went wrong and many events, by pure coincidence, worked against Flight 007: The first symptom was the deviation over the initial waypoints (*Cairn Mountain*,

Bethel), which, for whatever reason, were not queried by ATC. Then we have the parallel, at least initially, between the initial aircraft heading and the INS route. That heading, 245 degrees, took the aircraft toward the orbiting military RC-135, which, coincidentally, was leaving the Soviet radar screen at about the same time as the B-747 appeared on it. Finally, what sealed the fate of KAL 007 was the early morning darkness, which prevented any real visual identification of the aircraft, and the climb from 33,000 feet to 35,000 feet, just after the fighter aircraft fired a warning burst. KAL 007 is a complex tragedy, with a bizarre sequence of actions, and a lot of confusion – just like most accidents. But the real challenge is to learn from it and use it to prevent the accidents and incidents of the future. Nevertheless, many of the automated systems that we use today still suffer from the same problems that contributed to the navigation mishap of KAL 007. And as more and more automated systems are introduced into the cockpit and related systems, the problems of tracking what the automation is really doing are becoming more fundamental as ever before. Efforts are currently underway to develop engineering and human factors methods to identify these types of problems early on in the design phase.

REFERENCES

Abbott, K., Slotte, S. M., and Stimson, D. K. (1996). *The interface between flightcrews and modern flight deck systems*. Washington, DC: Federal Aviation Administration.

Degani A. and Heymann, M. (in press). Formal Verification of Human-Automation interaction. *Human Factors*.

International Civil Aviation Organization (1993). *Destruction of Korean Air Lines Boeing 747, on 31 August 1983*. Montreal, Quebec.

Wiener, E. L. (1989). The human factors of advanced technology ("glass cockpit") transport aircraft (NASA Contractor Report 177528). Moffett Field, CA: NASA Ames Research Center.

Woods, D., Sarter, N., and Billings, C. (1997). Automation surprises. In G. Salvendy (Ed.), *Handbook of human factors and ergonomics* (pp. 1926-1943). New York: John Wiley.

Figure 1. *Korean Air Lines Boeing 747-200.*

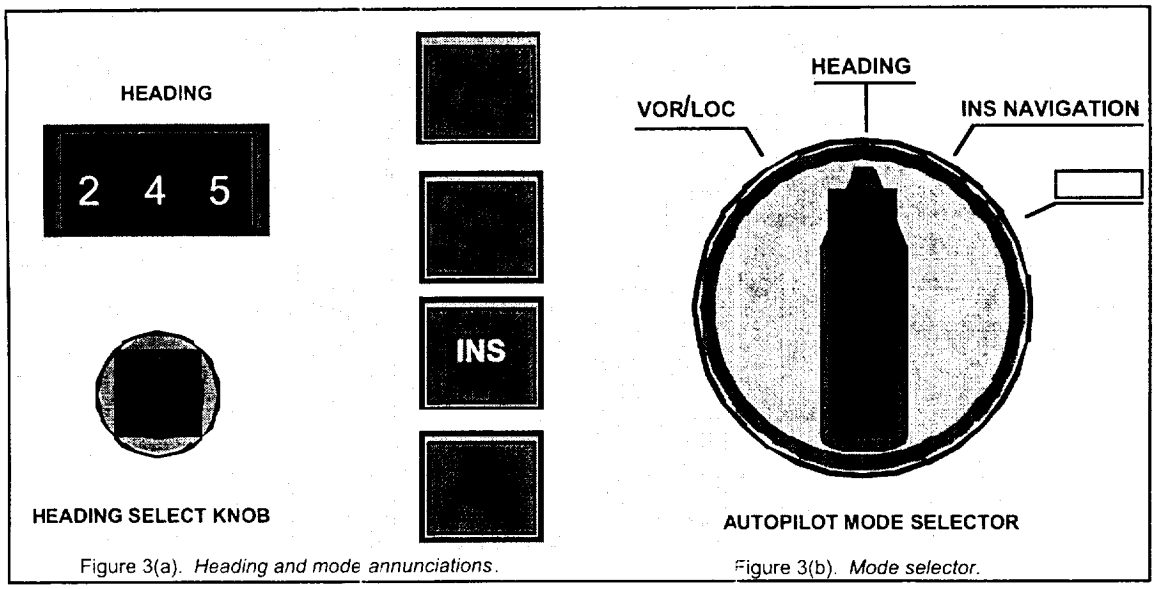

Figure 3(a). *Heading and mode annunciations.*

Figure 3(b). *Mode selector.*

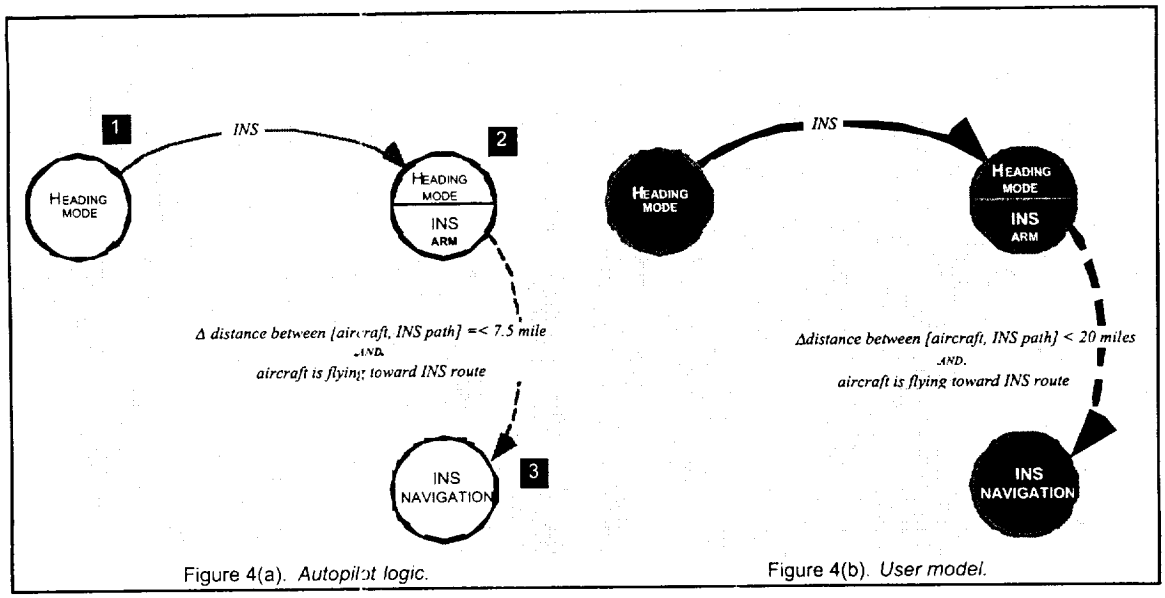

Figure 4(a). *Autopilot logic.*

Figure 4(b). *User model.*

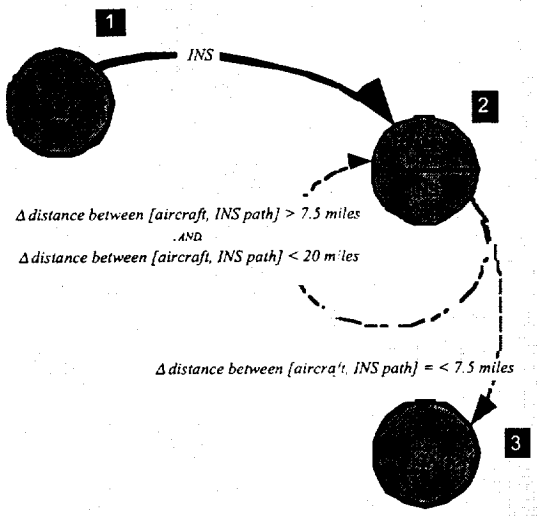

Figure 5(a). *The composite model.*

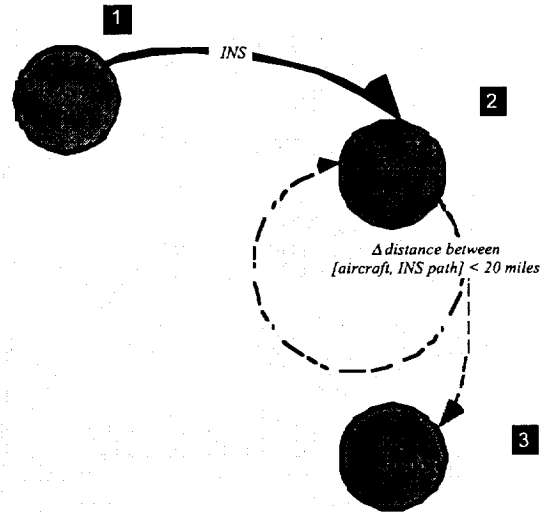

Figure 5(b). *The composite model from the user's view.*

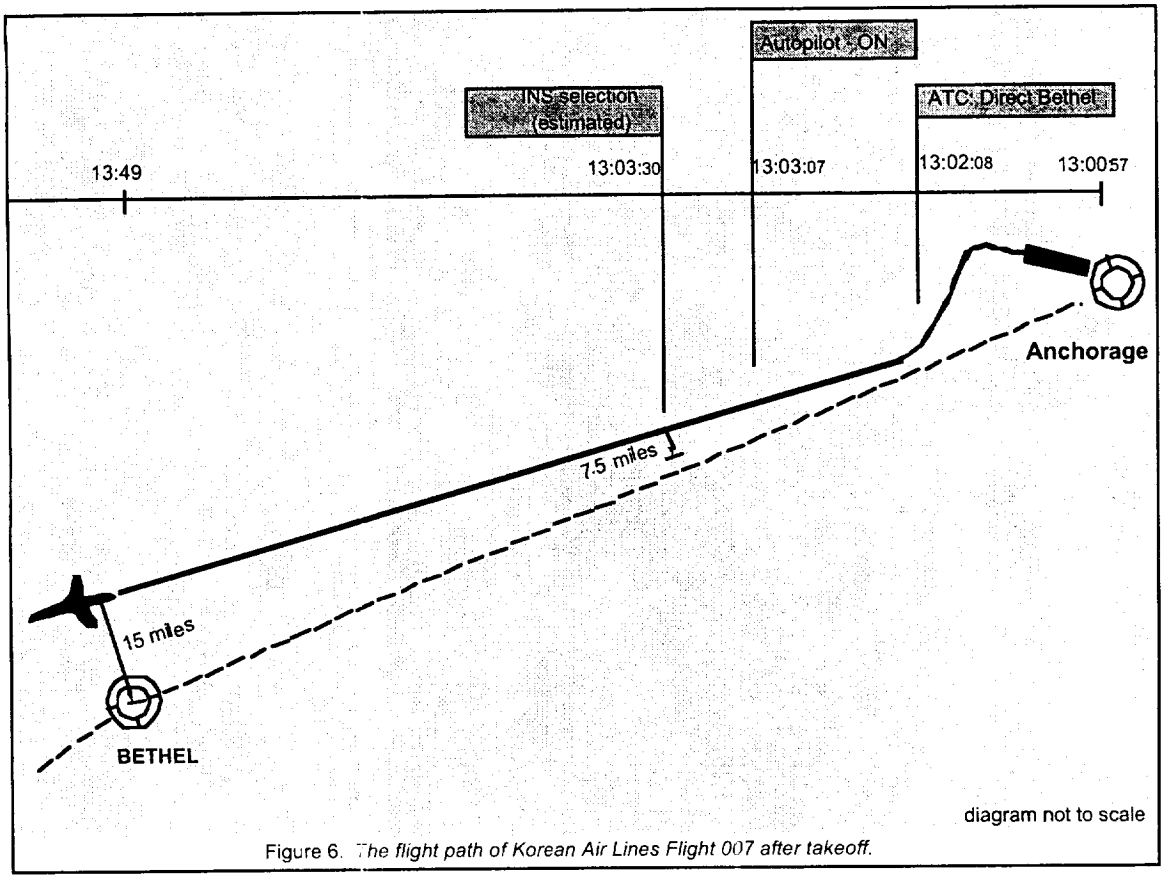

Figure 6. *The flight path of Korean Air Lines Flight 007 after takeoff.*

National Aeronautics and Space Administration

NASA Scientific and Technical Document Availability Authorization (DAA)

Use this form for all STI that is to be released outside of NASA. See Instructions on page 3.

☒ ORIGINAL ☐ MODIFIED

I. DOCUMENT/PROJECT IDENTIFICATION

TITLE	AUTHOR(S)
Korean air lines flight 007: Lessons from the past and insights for the future	Asaf Degani

ORIGINATING NASA ORGANIZATION *(Include organization code)*	PERFORMING ORGANIZATION *(If different)*
IC	

CONTRACT/GRANT/INTERAGENCY/PROJECT NUMBER(S)	DOCUMENT NUMBER(S)	DOCUMENT DATE
Aero Base RTOP 711-41-12		08/01/2001

CHECK: ☒ Conference ☐ Periodical ☒ Journal Name ☐ Book Title ☐ Publisher ☐ URL
and enter name, place, and date to right, if applicable.
Route through center or HQ Export Control Administrator.

also as a Journal paper (International Journal of Aviatoin Safety)
to be posted on WWW
and as presentations to the aviation community

II. NATIONAL SECURITY CLASSIFICATION *(Check one of the four boxes)*

☐ TOP SECRET ☐ SECRET ☐ CONFIDENTIAL ☒ UNCLASSIFIED

III. AVAILABILITY CATEGORY

(Author indicates ITAR or EAR, if appropriate. Author indicates USML or ECCN/CCL numbers, if known. Center or HQ Export Control Administrator must concur in Section VIII)

NASA EXPORT-CONTROLLED PROGRAM ST

☐ International Traffic in Arms Regulations (TAR)

☐ Export Administration Regulations (EAR)

Export-Controlled Document - U.S. Munitions List (USML Category) _____ or

Export Control Classification Number (ECCN) _____ from the

Commerce Control List (CCL) _____

CONFIDENTIAL COMMERCIAL STI *(Check appropriate box below and indicate the distribution limitation (see Additional Information and "Limited until (date)" if applicable):*

☐ TRADE SECRET

☐ Small Business Innovation Research (SBIR)

☐ COPYRIGHTED *(indicate appropriate distribution limitation (see Additional Information), if applicable).*

☐ Limited until *(date)*- if applicable _____

☐ Limited until *(date)*- if applicable _____

☐ Limited until *(date)*- if applicable _____

☐ Publicly available *(but subject to copying restrictions)*

ADDITIONAL INFORMATION *(Check appropriate distribution limitation below and/or limited until (date) above, if applicable).*

☐ U.S. Government agencies and U.S. Government agency contractors only

☐ U.S. Government agencies only

☐ NASA personnel & NASA contractors only

☐ NASA contractors and U.S. Government only

☐ NASA personnel only

☐ Available only with approval of issuing office: _____

☒ Publicly Available STI

Publicly available means it is unlimited and unclassified, is not export-controlled, does not contain confidential commercial data, and has cleared any applicable patent application.

9/171

IV. DOCUMENT DISCLOSING AN INVENTION

☐ If STI discloses an invention, Author/Originator must check box and send to Patent Counsel.

THIS DOCUMENT MAY BE RELEASED ON (date) _____

NASA HQ OR CENTER PATENT OR INTELLECTUAL PROPERTY COUNSEL SIGNATURE: Kathleen Wilson

DATE: 9/18/01

V. BLANKET AVAILABILITY AUTHORIZATION *(OPTIONAL)*

☐ This blanket availability authorization is granted on *(date)* _____
All documents issued under the following contract/grant/project number may be processed as checked in Sections II and III

CHECK ONE: ☐ Contract ☐ Grant ☐ Project Number _____

SIGNATURE _____

MAIL CODE _____

The blanket availability authorization granted on *(date)* _____ is

☐ RESCINDED - Future documents must have individual availability authorizations.

☐ MODIFIED - Limitations for all documents processed in the STI system under the blanket release should be changed to conform to blocks as checked in Sections II and III.

SIGNATURE _____

MAIL CODE _____ DATE _____

VI. AUTHOR/ORIGINATOR VERIFICATION

I HAVE DETERMINED THAT THIS PUBLICATION:

☐ DOES contain ITAR/export-controlled, confidential commercial information, and/or discloses an invention and the appropriate limitation is checked in Sections III and/or IV.

SIGNATURE _____

☒ Does NOT contain ITAR/export-controlled, confidential commercial information, nor does it disclose an invention and may be released as indicated above.

DATE 08/01/2001

VII. PROJECT OFFICER/TECHNICAL MONITOR/DIVISION CHIEF REVIEW OF I THRU VI

☒ APPROVED FOR DISTRIBUTION AS MARKED ☐ NOT APPROVED

NAME	MAIL CODE	SIGNATURE	DATE
M. SHAFTO	269-4	Mark D Shafto	9/4/01

VIII. EXPORT CONTROL REVIEW/CONFIRMATION

☒ Public release is approved

☐ Export-controlled limitation is approved

☐ Export-controlled limitation is not applicable

☐ Export-controlled limitation (ITAR/EAR marked in Section III is assigned to this document)

USML CATEGORY NUMBER	CCL NUMBER, ECCN NUMBER	CENTER OR HQ EXPORT CONTROL ADMINISTRATOR SIGNATURE	DATE
		Sonne Lan	9/5/01

IX. DAA FINAL APPROVAL

☒ APPROVED FOR DISTRIBUTION AS MARKED IF REQUIRED BY YOUR CENTER

SIGNATURE for Sonne Lan
Daniel Mancy

MAIL CODE IC DATE 9/5/01

☐ NOT APPROVED

X. DISPOSITION

SEND THIS FORM, WHEN COMPLETED, TO YOUR CENTER'S RESPONSIBLE OFFICE OR TECHNICAL PUBLICATIONS OFFICE.